



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,868	05/11/2006	Masaki Hamada	288056US40PCT	3257
22850	7590	03/18/2009		
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314				
EXAMINER				
CHAI, LONGBIT				
ART UNIT		PAPER NUMBER		
2431				
NOTIFICATION DATE		DELIVERY MODE		
03/18/2009		ELECTRONIC		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com  
oblonpat@oblon.com  
jgardner@oblon.com

### Office Action Summary

**Application No.**

10/578,868

**Applicant(s)**

HAMADA ET AL.

**Examiner**

LONGBIT CHAI

**Art Unit**

2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 27 February 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 16-24 and 26-28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 16-24 and 26-28 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 May 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

## DETAILED ACTION

1. Currently pending claims are 16 – 24 and 26 – 28.

### ***Response to Arguments***

2. Applicant's arguments with respect to instant claims have been fully considered but are moot in view of the new ground(s) of rejection necessitated by Applicant's amendment.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claim 16 and 28 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention of *a performance measuring device that sends a response request message*. Examiner notes any request message pending for a response is qualified as a response request message and, according to the disclosure of the instant application, it indicates "the performance abnormality detection condition includes the response time from transmission of a response request message to the communication device to reception of a response message to the response request message, and the number of times in which the response time exceeds the predetermined threshold" (SPEC: Page 7 / Line 25 – 30) and *there is no where in the*

*specification that a response request message need to be particularly sent from the performance measuring device besides the performance monitoring function.* Any other claims not addressed are rejected by virtue of their dependency.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 16 – 19, 21, 22, 24, 26 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanno et al. (U.S. Patent 2004/0064738), in view of Bang et al. (Korea KR-10-2004-0036228).

As per claim 16 and 28, Kanno teaches a denial-of-service attack detecting system for detecting a denial-of-service attack on a communication device, the denial-of-service attack detecting system comprising:

**a monitoring device that monitors each packet transmitted to the communication device and includes a traffic abnormality detecting unit that detects traffic abnormality information indicating an abnormality of traffic based on packets transmitted to the communication device** (Kanno: Figure 1 / Element 103 (a proxy) & Figure 2 / Element 203 and 205, Para [0040] Line 1 – 2, Para [0032] Line 10 – 11, Para [0036] Line 16 – 19, Para [0038] Line 6 – 11 and Para [0044] Line 12 – 14: (a) "Number of Data Requests Measurement Unit" monitors the number of data requests transmitted on the link (b) a portion of "Response

Probability Calculation Unit" determines in a case where the load on this occasion is extraordinary heavy (or contributed as the number of pending data requests @ traffic is extraordinary large) that the server may be under a DoS attack (i.e. abnormality situation) and therefore (c) the "Number of Data Requests Measurement Unit" and part of the "Response Probability Calculation Unit" are qualified as an integral part of a monitoring device that manages the data request portion of the traffic);

**a performance measuring device that measures response performance of the communication device by sending a response request message and is separate from the communication device and the monitoring device, the performance measuring device including a performance abnormality detecting unit that detects performance abnormality information indicating an abnormality of throughput of the communication device** (Kanno: Figure 1 / Element 103 (a proxy) & Figure 2 / Element 204 and 205, Para [0040], Para [0032], Para [0036], Para [0038], Para [0044] and Para [0050] Line 3 – 8: (a) "Number of Data Supplies (i.e. Response) Measurement Unit" monitors the number of data responses received from the link, (b) a portion of "Response Probability Calculation Unit" determines in a case where the load on this occasion is extraordinary heavy (or contributed as the number of completed data responses is extraordinary small) that the server may be under a DoS attack (i.e. abnormality situation) and therefore (c) the "Number of Data Supplies (i.e. Response) Measurement Unit" and part of the "Response Probability Calculation Unit" are qualified as an integral part of performance measuring device that manages the data response portion corresponding to the request packets. **Examiner notes**, besides, any request message pending for a response is qualified as a response request message and tracking, on the "Response Probability Calculation Unit", the correspondence between a data request and a certain data response by transferring a data request via a "data request transfer unit" can be

considered as "sending a response request message which is separate from the communication device and the monitoring device", as recited in the claim (*Kanno: Para [0050] Line 3 – 8*)).

**the attack determining device including an effects determining unit that determines whether the communication device has received the denial-of-service attack, using both the traffic abnormality information and the performance abnormality information** (Kannon: Figure 1 & Para [0040] Line 7 – 8, Para [0061], Para [0036], [0044] and [0045]: the Server Security Protection Apparatus judges the server may be under a DoS attack (i.e. abnormality situation) based upon a probability of load ratio associated with a combined effect contributed not only by the number of pending data requests @ traffic (e.g. extraordinary large) but also by the number of completed data responses (e.g. extraordinary small)).

**the effects determining unit determining that the communication device has received the denial-of-service attack, when it is determined that one of the traffic abnormality information and the performance abnormality information causes an occurrence of one of the traffic abnormality information and the performance abnormality information based on an abnormality occurrence time included in the traffic abnormality information and the performance abnormality information** (Kannon: Figure 1 & Para [0040] Line 7 – 8, Para [0061], Para [0036] Line 11 – 12, [0044] Line 12 – 14 and [0045]: an abnormality situation (e.g. a DoS attack) is detected according to an extraordinary heavy load within a pre-determined time period between the pending data requests and the completed data responses, as taught by Kannon, which can be considered as an abnormality occurrence time).

However, Kanno does not disclose expressly an attack determining device that is connected to and performs communication with the monitoring device and the performance measuring device.

Bang teaches **an attack determining device that is connected to and performs communication with the monitoring device and the performance measuring device** (Bang: Abstract: a *separate* active security management system communicates with a "monitoring unit" and a "harmful traffic tracking unit", which is qualified as an attack determining device).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bang within the system of Kannon because (a) Kannon teaches detecting a denial of service attack on the server based upon the performance level of load state of the data request / response traffic (Kannon: Abstract), and (b) Bang teaches providing a security mechanism where a traffic monitoring unit and a harmful traffic tracking unit can monitor a harmful traffic event (such as denial of service attack) based on a threshold criteria whether exceeding a pre-set reference value and communicate the security event to an active security management system (Bang: Abstract).

As per claim 17, Kanno as modified teaches the monitoring device further includes a traffic-abnormality-information transmitting unit that transmits the traffic abnormality information to the attack determining device (Bang: Abstract: the monitoring device transmitting the event to the security management device).

As per claim 18, Kanno as modified teaches the performance measuring device further includes a performance-abnormality-information transmitting unit that transmits the performance abnormality information to the attack determining device (Kannon: Figure 9 and Para [0152]: the transmitting unit of the processing situation reception unit transmits the performance abnormality information to the server computer protection apparatus for decision making on DoS attack).

As per claim 19, Kanno as modified teaches the traffic abnormality detecting unit detects the traffic abnormality information based on a predetermined attack detection condition that is set in advance (Bang: Abstract: a traffic monitoring unit periodically monitors traffic change against a pre-set reference value and detects an IP packet having the traffic component exceeding the pre-set reference value).

As per claim 21, Kanno as modified teaches the traffic abnormality detecting unit detects the traffic abnormality information based on a steady traffic indicating an average traffic of the packet transmitted to the communication device (Bang: Abstract).

As per claim 22, Kanno as modified teaches the performance abnormality detecting unit detects the performance abnormality information based on a predetermined performance abnormality detection condition that is set in advance (Kanno: Para [0044]).

As per claim 24, Kanno as modified teaches the performance abnormality detecting unit detects the performance abnormality information based on a steady performance indicating an average performance feature of the communication device (Kanno: Para [0143] Line 7 – 9: a processing situation reception unit measures the performance (traffic load) of the server is on an average level of traffic load).

As per claim 26, Kanno as modified teaches when the effects determining unit determines that the communication device received the denial-of-service attack, the attack determining device transmits the traffic abnormality information and the performance abnormality information used for the determination to a device for reporting to an operator

(Bang: Abstract: the monitoring device transmitting the event to the security management device).

5. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kanno et al. (U.S. Patent 2004/0064738), in view of Bang et al. (Korea KR-10-2004-0036228), and in view of Ioele et al. (U.S. Patent 7,007,299).

As per claim 20, Kanno as modified does not disclose expressly a signature generating unit that generates a signature indicating a feature of the packet attacking the communication device, based on the attack detection condition, and the traffic abnormality information includes the signature.

Ioele teaches a signature generating unit that generates a signature indicating a feature of the packet attacking the communication device, based on the attack detection condition, and the traffic abnormality information includes the signature (Ioele: Column 6 Line 34 – 41 / Line 49 – 55: the intrusion detectors monitor network traffic for attack signatures and alert a security manager when an attack is detected).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ioele within the system of Kannon as modified because (a) Kannon teaches detecting a denial of service attack on the server based upon the performance level of load state of the data request / response traffic (Kannon: Abstract), and (b) Ioele teaches providing a traffic monitoring unit for detecting a denial of service attack by running on a dedicated host and monitor network traffic for attack signatures and alert a security manager when an attack is detected (Ioele: Column 6 Line 34 – 41 / Line 49 – 55).

6. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kanno et al. (U.S. Patent 2004/0064738), in view of Bang et al. (Korea KR-10-2004-0036228), and in view of Patrick et al. (U.S. Patent 7,310,684).

As per claim 23, Kanno as modified does not disclose expressly the performance abnormality detection condition includes a response time from transmission of a response request message to the communication device to reception of a response message corresponding to the response request message, and number of times that the response time exceeds a predetermined threshold.

Patrick teaches the performance abnormality detection condition includes a response time from transmission of a response request message to the communication device to reception of a response message corresponding to the response request message, and number of times that the response time exceeds a predetermined threshold (Patrick: Column 25 Line 24 – 27 and Column 24 Line 10 – 12: an average response time exceeding a threshold value for a DoS attack).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Patrick within the system of Kannon as modified because (a) Kannon teaches detecting a denial of service attack on the server based upon the performance level of load state of the data request / response traffic (Kannon: Abstract), and (b) Patrick teaches providing a traffic monitoring unit for detecting a denial of service attack by detecting an average response time exceeding a threshold value on a DoS attack (Patrick: Column 25 Line 24 – 27 and Column 24 Line 10 – 12).

7. Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kanno et al. (U.S. Patent 2004/0064738), in view of Bang et al. (Korea KR-10-2004-0036228), and in view of Costa et al. (U.S. Patent 2007/0006314).

As per claim 27, Kanno as modified does not disclose expressly each of the traffic abnormality information and the performance abnormality information includes a certificate, and the effects determining unit determines whether the communication device received the denial-of-service attack, after performing an authorization based on certificates.

Costa teaches each of the traffic abnormality information and the performance abnormality information includes a certificate, and the effects determining unit determines whether the communication device received the denial-of-service attack, after performing an authorization based on certificates (Costa: Para [0142]: verify the signature of a message using the certificate to authenticate the message sending device in order to reduce the occurrence and/or effect of denial of service attack to the network).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Costa within the system of Kannon as modified because (a) Kannon teaches detecting a denial of service attack on the server based upon the performance level of load state of the data request / response traffic (Kannon: Abstract), and (b) Costa teaches providing an improved method to reduce the occurrence and/or effect of denial of service attack to the network by verifying the signature of a message using the certificate to authenticate the message sending device (Costa: Para [0142]).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai E.E. Ph.D  
Primary Examiner, Art Unit 2431  
03/10/2009